July 22, 2016

North Dakota State and Local Intelligence Center

Bi-Weekly Cyber Rollup

Included in this week's summary:
Click on the Section Header to go directly to that location in the Summary

NORTH DAKOTA & REGIONAL

(U) Cybersecurity task force looks to legislation, insurance

(U) An interim task force is undertaking development of procedures for responding to data breaches involving state IT networks – and it may go so far as to recommend cyber insurance, which has become increasingly expensive.

Source: (U) http://bismarcktribune.com/news/state-and-regional/cybersecurity-task-force-looks-to-legislation-insurance/article_7e4172c1-28fb-58f2-9047-cffb3abeec63.html#utm_source=bismarcktribune.com&utm_campaign=%2Femail-updates%2Fdaily-headlines%2F&utm_medium=email&utm_content=DE901923662317836E9F9DE9D1AF02B58FB898D8

(U) Dayton wants big boost in cybersecurity funding; lawmakers won't click

(U) Spear phishing, botnet armies, cyber disruptors – that's just a sampling of the attacks creating constant worry for Christopher Buse, Minnesota's chief information security officer. Countless times a day, hackers try to find and exploit gaps in Minnesota's vast state government computer network, hoping to steal sensitive information or gum up operations. The system also encounters state employees wading into data pools where they probably do not belong.

Source: (U) http://www.mprnews.org/story/2016/04/21/dayton-bid-to-boost-minnesota-cybersecurity-sputters

NATIONAL

(U) Ex-Cards scouting director Chris Correa sentenced to prison for hacking Astros

(U) A federal judge sentenced the former scouting director of the St. Louis Cardinals to nearly four years in prison Monday for hacking the Houston Astros' player-personnel database and email system in an unusual case of high-tech cheating involving two Major League Baseball clubs.

Source: (U) http://espn.go.com/mlb/story/_/id/17101079/chris-correa-former-st-louis-cardinals-scouting-director-sentenced-jail-hacking-houston-astros

(U) Why lawmakers are trying to make ransomware a crime in California

(U) State legislation to outlaw ransomware is drawing broad support from tech leaders and lawmakers, spurred by an uptick in that type of cybercrime and a series recent attacks on hospitals in Southern California

Source: (U) http://www.latimes.com/politics/la-pol-sac-crime-ransomware-bill-20160712-snap-story.html

(U) Malwarebytes Puts NASCAR Team Back In The Driver's Seat After A Ransomware Attack

(U) Dave Winston is the crew chief for the NASCAR racing team TISI +% Circle Sport-Levine Family Racing. Around lunchtime on April 5th he got a phone call from race team engineer Kevin Walter who wanted to know what was going on with all the communication between Winston's computer and their Dropbox account. Winston wasn't using his computer and didn't know what Walter was talking about. Walter told him to get his computer offline. Fast. Winston took his system off the network and then a window no one wants to see popped up on his screen. Circle Sport-Levine Family Racing had been hit by a ransomware attack.

Source: (U) http://www.forbes.com/sites/kevinmurnane/2016/06/24/malwarebytes-puts-nascar-team-back-in-the-drivers-seat-after-a-ransomware-attack/#3eeb7b423163

(U) The Troubling State of Security Cameras; Thousands of Devices Vulnerable

(U) The recent Lizard Squad hack which resulted in a lot of CCTV cameras targeted and hijacked by a DDOS attack has highlighted the need for better security cameras. A study conducted by Protection1 shows how many security agencies do not take things seriously.

Source: (U) https://www.hackread.com/thousands-of-security-cameras-vulnerable/

INTERNATIONAL

(U) Oracle's critical patch update for July contains record number of fixes

(U) Oracle released its July Critical Patch Update (CPU) that addressed a total of 276 vulnerabilities in several of its products including 19 critical security flaws affecting the Oracle WebLogic Server component, the Hyperion Financial Reporting component, and the Oracle Health Sciences Clinical Development Center component, among other applications. The update also resolves 36 security flaws in applications specifically designed for the insurance, health, financial, and utility sectors, as well as 159 remote code execution (RCE) flaws that can be exploited without authentication.

Source: (U) http://www.securityweek.com/oracle-addresses-276-security-flaws-19-criticaljuly-2016-cpu

(U) Free decrypter available for Bart ransomware

(U) A security researcher for AVG released a free decrypter for the Bart ransomware that recovers files locked by the ransomware after discovering Bart uses one password for all files placed inside a password-protected ZIP archive.

Source: (U) http://news.softpedia.com/news/free-decrypter-available-for-bart-ransomware506469.shtml

(U) Gmail security filters can be bypassed just by splitting a word in two

(U) Security researchers from SecureState discovered that an attacker can bypass Gmail's security features responsible for detecting malicious macros in Microsoft Office document attachments by separating "trigger words" into two words or across a row of text after finding that the security filters failed to detect malicious macros in the script when an attacker split a sensitive term on two different lines of the exploit code.

Source: (U) http://news.softpedia.com/news/gmail-security-filters-can-be-bypassed-just-bysplitting-a-word-in-two-506447.shtml

(U) Apple patches tens of vulnerabilities in iOS, OS X

(U) Apple Inc., released security updates for several of its products including OS X El Capitan version 10.11.6, which patched a total of 60 security bugs affecting components such as audio, FaceTime, and CFNetwork, among others after a Zscaler researcher discovered the flaws could allow unprivileged applications to access cookies stored in the Safari browser. Apple also released iOS version 9.3.3., resolving 43 vulnerabilities, one of which could allow an attacker with physical access to the device to abuse Siri and view private contact information, among other patches.

Source: (U) http://www.securityweek.com/apple-patches-tens-vulnerabilities-ios-os-x

(U) CryptXXX now being distributed via spam emails

(U) Security researchers from Proofpoint warned that the CryptXXX malware was leveraging a spam email campaign after discovering that the emails, using subjects such as "Security Breach – Security Report #123456789," were tricking users into activating malicious macros embedded in the emails' document attachments, which were designed to download and install the ransomware when the victim interacted with them.

Source: (U) http://www.securityweek.com/cryptxxx-now-being-distributed-spam-emails

(U) Juniper patches high-risk flaws in Junos OS

(U) Juniper Networks fixed several vulnerabilities in the Junos operating system (OS) used on its networking and security appliances, including an information leak in the JWeb interface, vulnerabilities that could lead to denial of service conditions, a potential kernel crash, a potential memory buffer (mbuf) leak, a crypto vulnerability, and an issue with SRX Series devices.

Source: (U) http://www.networkworld.com/article/3095812/juniper-patches-high-riskflaws-in-junos-os.html